

What is claimed is

1 1. A cryptography method, comprising:
2 determining information to be encrypted; and
3 encrypting said information using an arithmetic which is
4 not associative.

1 2. A method as in claim 1, wherein said encrypting
2 comprises using a non-trivial ci-quasigroup to encode.

1 3. A method as in claim 2, further comprising decoding
2 using the crossed-inverse function of said ci-quasigroup.

1 4. A method as in claims 1 or 2, wherein said encrypting
2 comprises carrying out a first encryption to get a first
3 result, then carrying out a second encryption using said first
4 result, and encryption can be iterated an arbitrary number of
5 times.

1 5. A method as in claim 2 further comprising defining a
2 rule indicative of said quasigroup.

1 6. A method as in claim 3 further comprising defining a
2 rule indicative of said crossed inverse of said quasigroup.

1 7. A method as in claim 1 further comprising carrying

002250-052200

1 15. A method as in claim 14 wherein said block cipher
2 are defined by a function.

1 16. A method as in claim 14 wherein said block ciphers are
2 formed using cross inversed quasigroups, used according to $C =$
3 $f(M, K)$ for the encryption and $M = f_{inv}(C, K)$ for the decryption.

1 17. A method as in claim 1 wherein said encrypting uses
2 XIP neofields.

1 18. A method as in claim 1 wherein said encrypting uses
2 near rings.

1 19. A cryptography method, comprising:
2 determining information to be encrypted; and
3 encrypting said information using an arithmetic which is not
4 commutative.

1 20. A method as in claim 19, wherein said encrypting
2 comprises using a quasigroup to encode.

1 21. A method as in claim 19, further comprising decoding
2 using a crossed inverse of said quasigroup.

1 22. A method as in claim 1, wherein said encrypting
2 comprises carrying out a first encryption to get a first

002250-0659450

3 result, then carrying out a second encryption using said first
4 result.

1 23. A cryptography method comprising encrypting
2 information using an arithmetic with an algebraic structure,
3 said algebraic structure being a nongroup, nonfield structure.

1 24. A method as in claim 23 wherein said algebraic
2 structure is not associative.

1 25. A method as claim 23 wherein said algebraic
2 structure is not commutative.

1 26. A method as in claim 24 wherein said algebraic
2 structure is not commutative.

1 27. A method as in claim 23 wherein said arithmetic is a
2 crossed inverse quasigroup.

1 28. A method as in claim 24 wherein said method uses a
2 near ring.

1 29. An apparatus comprising a program stored on a
2 computer readable media including instructions to:
3 encrypt a message using a non-associative arithmetic; and
4 send the encrypted message.

002250" 86597560

1 30. An apparatus as in claim 29, wherein said arithmetic
2 includes a non-trivial crossed inverse quasigroup.

1 31. An apparatus as in claim 29, wherein said arithmetic
2 is one which is based on a multiplication table which is
3 expressed as a rule.

1 32. An apparatus as in claim 29, further comprising
2 adding a random seed to said arithmetic.

1 33. An apparatus as in claim 30, further comprising
2 using an additional encryption to provide an effective key
3 size of x^2 of the original encryption.

1 34. A method of encrypting in a computer, comprising:
2 obtaining, in the computer, a file to be encrypted;
3 using a non-associative arithmetic to encrypt the file;
4 and
5 using another non-associative arithmetic to further
6 encrypt the once-encrypted file.

002250" 86597500